

Instructions for Developing Policies and Procedures to Implement HIPAA's Administrative Requirements

45 CFR 164.530

PURPOSE: To establish the policy and procedure on the Administrative requirements of the Health Insurance Portability & Accountability Act (HIPAA).

POLICY: IHS shall formulate policies and procedures in accordance with local policies and procedures and HIPAA to implement the provisions of this Section.

PROCEDURES: The following procedures will be used to ensure compliance with HIPAA regulation at the Service Unit level.¹

1. Designation of Privacy Official and Contact Person

Each IHS facility shall designate a Privacy Official (Officer) and/or a contact person who shall be responsible for development of local policies and procedures for HIPAA compliance within the Service Unit area. The Privacy Officer and the contact person can be the same individual. The Privacy Officer and/or contact person must be knowledgeable and able to provide information covered in the IHS Notice of Privacy Practices and receive complaints and possibly resolve HIPAA issues. .

2. Training

IHS facilities must provide initial HIPAA overview training to all employees, volunteers and onsite contractors. New employees must receive training as soon as possible, but no later than 30 days after entering on duty. Function specific training must also be provided to other categories of staff such as Health Information Management staff, Business Office, and Nursing & Medical Staff. Training must also be provided to designated staff when policies & procedures are revised. Training provided to staff shall be documented and maintained in writing or electronically for six years.

3. Safeguards

IHS facilities shall put in place policies and procedures to safeguard PHI in accordance with the Privacy Act and HIPAA regulations for both electronic and paper records to include administrative, technical and physical safeguards.

- Examples: Administrative Safeguards includes orientation and termination policies, incident reporting policies, access, contingency and disaster recovery.
- Examples: Technical Safeguards: User access and restrictions, user monitoring, authentication, and password issuance.
- Examples: Physical Safeguards: Physical access control during and after hours, shredding policies, and health record removal from facility.

¹ For Areas that provide CHS directly through the Area Office, references to the Service Unit level and the facility should be considered references to the Area CHS Office, as applicable.

4. Complaints:

All complaints regarding HIPAA and Privacy Act violations shall be addressed to the Service Unit Director/Chief Executive Officer or designee. The complaints must be documented, maintained, filed and a brief explanation of resolution, if any.

Note: Individuals can file complaints directly to the Secretary, DHHS.

5. Sanctions

IHS facilities shall develop policies and procedures using current IHS policies and procedures, including employee Standards of Conduct (5 CFR Part 3635), Privacy Act (45 CFR Appendix A – Part 5b) and the HIPAA Privacy Rule (45 CFR Part 164). The Human Resources Office could be helpful with this policy. Sanctions could range from warning to termination depending on the level of violation. Employees must be made aware of these policies and procedures during training. Facilities must document the sanctions that are applied, if any.

IHS and its facilities shall not invoke sanctions against employees, volunteers and onsite contractors under the following conditions:

- A. Whistleblower - if an employee discloses PHI provided s/he believes in good faith that the facility is in violation of HIPAA or other clinical or health care standards, or that facility activities or conditions could potentially endanger one or more patients, workers or members of the public, to:
 - A health oversight authority or public health authority authorized by law to investigate such violations or accreditation organization for the purpose of reporting the failure to meet standards or misconduct by an IHS facility; or
 - An attorney retained by the employee for the purpose of determining his or her legal options with regards to an IHS facility's conduct.
- B. Disclosure by employees who are victims of a crime to a law enforcement official provided that PHI disclosed is about the suspected criminal and PHI disclosed is limited to the following:
 - a. Name and address
 - b. Date and place of birth
 - c. Social security Number
 - d. ABO blood type and Rh factor
 - e. Type of injury
 - f. Date and time of treatment
 - g. Date and time of death, if applicable
 - h. A description of distinguishing physical appearance including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos.

6. Mitigation

When IHS facility becomes aware of possible violation of the use or disclosure of PHI by its employee or business associate, the facility shall take reasonable steps to ensure mitigation of the disclosure or violation. For example, when PHI has been improperly disclosed, steps shall be taken to mitigate its improper use based on knowledge on how such information might be used.

7. Refraining from Intimidating or Retaliatory acts

IHS shall not intimidate, threaten, coerce, discriminate against, or take retaliatory action against patients for exercising their rights under the HIPAA Privacy Rule, or against any person including employees, volunteers, and onsite contractors, for participating in any process established for:

- filing privacy complaints with the Secretary, DHHS
- testifying, assisting or participating in an investigation, compliance review, proceeding, or hearing related to the Privacy Rule
- opposing any act or unlawful practice under the Privacy Rule and the manner of opposition is reasonable and does not involve a disclosure of PHI not permitted

8. Waiver of rights

IHS facilities shall not require individuals to waive their rights under the HIPAA Privacy Rule, including but not limited to their rights to file complaints with the Secretary, as a condition for the provision of treatment, payment, eligibility (CHS), or other benefits.

9. Policies and Procedures, and Documentation

IHS shall develop policies and procedures in each of the relevant section of the HIPAA Privacy Rule and a process shall be established for revisions to reflect future changes.